FILED LOC
RECEIVED COP
APR 29 2019
19-8792MB
CLERK US DISTRICT COURT
DISTRICT OF ARIZONA
BY DEP

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Bradley Gittus, being duly sworn, depose and state as follows, to wit:

PRELIMINARY BACKGROUND INFORMATION

1. I am a Special Agent (SA) with Homeland Security Investigations (HSI) assigned to the Office of the Assistant Special Agent in Charge, Douglas, Arizona. I have been so employed since September 2015. I graduated from Criminal Investigator Training Program and Homeland Security Special Agent training at the Federal Law Enforcement Training Center. While there I received specific training on cybercrimes where computers and the internet are used in the sexual exploitation of children, including (but not limited to) violations of 18 U.S.C. Sections 2252 and 2252A, which prohibit a person from knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, child pornography, as defined in 18 U.S.C. Section 2256(8). I have received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children. In addition, I have been involved in and conducted numerous investigations relating to child pornography and online child exploitation, which have included participation in searches and seizures of child pornography, including computers and digital media, the arrests and interviews of subjects in said investigations, and the forensic examination of digital evidence obtained in said investigations. The statements contained in this Affidavit are based on my experience and background as a Special Agent and on information provided by other law enforcement agents.

2. I make this affidavit in support of an application for a search warrant on the following item, which was seized from Scott HAMSHER on February 16, 2019, after a consensual interview at the Sierra Vista Police Department:

One (1) Samsung Galaxy S7 edge SM-G935T and all internal memory therein (Hereinafter "SUBJECT DEVICE.")

3. The purpose of this application is to seize and search evidence, more particularly described in Attachment A, of violations of 18 U.S.C. §§ 2422(b), which make it a crime to knowingly attempt to persuade, induce, entice, and coerce an individual who has not attained the age of eighteen to engage in sexual activity for which any person can be charged with a criminal offense.

4. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2422(b) is located within the SUBJECT DEVICE utilized by Scott Eugene HAMSHER (hereinafter "SUBJECT").

5. The SUBJECT DEVICE to be searched is currently in the possession of Homeland Security Investigation agents.

6. No prior attempt by investigative or legal process has been submitted to obtain the same or similar information sought in this warrant application.

PERTINENT FEDERAL CRIMINAL STATUTES

7. This investigation concerns alleged violations of 18 U.S.C. §§ 2422(b), which make it a crime to knowingly attempt to persuade, induce, entice, and coerce an individual who has not attained the age of eighteen to engage in sexual activity for which any person can be charged with a criminal offense.

DEFINITIONS

8. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B:

a. Cellular telephone: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the devices.

b. Digital device includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communications devices such as modems, cables and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips; and security devices.

c. Computer refers to an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to

or operating in conjunction with such device. *See* 18 U.S.C. 1030(e)(1).

d. Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic or other digital form. It commonly includes computer operating systems, applications and utilities.

f. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.

g. Computer passwords and data security devices consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software of digital code may include programming code that creates test keys or hot keys, which perform certain pre-set security functions when touched. Data security

software or code may also encrypt, compress, hide or booby-trap protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

h. Digital camera: A digital camera is a device that records still and moving images digitally. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

i. Child Pornography is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. 2256(8).

j. Child Erotica refers to materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. *See Kenneth V. Lanning, Child Molesters: A Behavioral Analysis* (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. *See United States v. Cross*, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual

photographs of children admissible to show intent and explain actions of defendant); *United States v. Caldwell*, No. 97-5618, 1999 WL 238655 (E.D. Ky. Apr. 13, 1999) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

k. Visual depictions include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. 2256(5).

l. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. Internet Service Providers or ISPs are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account.

n. IP Address: "Internet Protocol address or IP address refers to a unique number used by a computer or other device to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different

unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. Internet Service Providers maintain logs of which subscriber was issued a particular IP address at any particular time.

o. ISP Records are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISPs servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

p. Minor means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

q. Sexually explicit conduct means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

r. The terms records, documents and materials include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives,

videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

s. Image or copy refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN

9. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who have a sexual interest in children, and in images of children, have certain characteristics:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or

drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS IN CHILD EXPLOITATION INVESTIGATION

10. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the SUBJECT DEVICE, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the SUBJECT DEVICE for at least the following reasons:

a. Individuals who engage in criminal activity, including the sexual abuse of children, use digital devices, like the SUBJECT DEVICE, to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device, documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; and/or contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social media accounts.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating

their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

11. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used them (or did not), and when. Based on my knowledge, training, and

experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in the SUBJECT DEVICE at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the SUBJECT DEVICE, not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point

toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a

particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to facilitate the trafficking or sex trafficking of a minor, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

FACTS OF THE INVESTIGATION

12. Homeland Security Investigations Douglas, Arizona ("HSI Douglas"), Child Exploitation Group ("CEG") Special Agents ("SA") have been monitoring various websites to identify individuals sexually exploiting children. Website A[1] is a website designed for adults to find sexual partners, but is known to law enforcement as having members actively sexually exploiting children as well. Specifically, in connection with this warrant, HSI Douglas agents, acting in an undercover (UC) capacity, identified and had contact with an individual who confirmed his willingness to sexually abuse a child.

[1] In the interest of protecting ongoing investigations involving the website, your Affiant will not list it here.

13. On or about February 16, 2019, HSI agents accessed Website A posing as a 14-year-old girl in the Sierra Vista, Arizona area and were solicited by an account, "drtyknkyfn," (herein "HAMSHER"). HAMSHER's profile picture was an erect penis.

14. On February 16, 2019, after learning that the UC with whom he was chatting was a 14 year-old girl, HAMSHER asked the UC about her sexual interests, past sexual experiences, and the prospects of engaging in sexual acts.

15. On February 16, 2019, the UC requested to continue their conversation via cellphone text messaging. HAMSHER agreed and continued his conversation with the UC agent via text message, continuing to discuss sexual conduct with the UC. For example, HAMSHER stated: "I want to come taste you baby girl" and "I already told my kids I was going to leave for a couple hours." After expressing concern about whether the UC was a police officer (and being assured she was not), HAMSHER planned to meet the UC to later that evening.

16. HAMSHER arrived at the agreed upon location in Sierra Vista, Arizona on February 16, 2019, as planned. HSI Special Agents observed a grey sedan pull into the parking lot where he parked and remained in the car with the engine running. While waiting for the 14-year-old to arrive, HAMSHER sent two text messages to the UC, first writing "I am here" followed by "where are you?" four minutes later.

17. HAMSHER was taken into custody, and after waiving his Miranda rights, HAMSHER stated that he came to the meet location for the purpose of having sex with the underage minor. HAMSHER, who had condoms in his possession, admitted that he knew the girl he was meeting was under the age of 18 and stated that her age didn't matter to him when he was planning to meet her.

18. When he was arrested, HAMSHER had the SUBJECT DEVICE in his possession. The SUBJECT DEVICE is currently in the lawful possession of Homeland Security

Investigations (HSI) and stored at 2334 East Highway 80 Douglas, AZ 85635.

CONCLUSION

19. Because HAMSHER used the SUBJECT DEVICE to communicate with the UC via text, and may also have used the SUBJECT DEVICE to Website A and chat with the UC, as well as to post the above-mentioned photograph of his penis, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of criminal offenses, in violation of 18 U.S.C. §§ 2422(b), may be located in the SUBJECT DEVICE and respectfully request that a warrant issue for the search and seizure of those items described in Attachments A and B.

Respectfully submitted,

Bradley Gittus, Special Agent
Homeland Security Investigations
Douglas, Arizona

Subscribed and sworn to before me
on this 26th day of April, 2019

Honorable D. Thomas Ferraro
United States Magistrate Judge